REMARKS

Claims 1-9, 11, 13-54, 56-81, and 83 are pending in this application. Claims 10, 12, 55, and 82 have been previously canceled. Applicant has amended claims 28, 51, and 69 to more particularly point out and distinctly claim Applicant's invention and to address typographical and/or stylistic issues. No new matter has been introduced by way of these amendments.

As a preliminary matter, Applicant notes that the Examiner has not rejected claims 16-26, 31, 41-49, 65, 70, or 80 over any prior art reference or under any statutory basis. Applicant therefore believes that the unaddressed claims are in condition for allowance.

Rejections Under 35 U.S.C. § 112

The Examiner has rejected claims 28, 51, and 69 under 35 U.S.C. § 112, second paragraph as indefinite. Specifically, with respect to claims 28 and 51, the Examiner has maintained his assertion of the prior Office Action, mailed October 25, 2005, that independent claim 3 recites that the locations in the protected space must remain unaltered, but that claim 28, which depends on claim 3, recites the alteration of data in the protected space. The Examiner concludes that these aspects are contradictory to one another, thereby rendering claim 28 indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. The Examiner makes a similar argument with respect to claim 51. (Office Action, dated May 26, 2006, pp. 2-4, hereinafter "Office Action".)

As a preliminary matter, Applicant thanks the Examiner for his analysis and suggested claim amendments.

Applicant has amended claims 28 and 51 to better illustrate how aspects of those claims and their respective parent claims are complimentary and not inconsistent. Specifically, Applicant has amended claim 28 to recite "*after the computer system is restarted from the powered-down state*, copying the saved data from the redirected space to associated locations in the protected space, thereby making permanent the data that was redirected to the redirected space" (emphasis added). Claim 3, from which claim 28 depends, recites "the data stored in the

protected space automatically remains unaltered *when the computer system is restarted from a powered-down state*" (emphasis added). Read in conjunction with claim 3, claim 28 recites an additional aspect of copying the saved data (of claim 27) to associated locations in the protected space, with the additional aspect of copying the saved data occurring *after* the computer system is restarted from the powered-down state. The additional aspect recited by claim 28 is complimentary to, and not inconsistent with, the aspect that data automatically remains unaltered when the computer system is restarted from a powered-down state, as recited by claim 3. Specifically, claim 28 recites an additional operation of altering the (initially) unaltered data by copying data from the redirected space to associated locations in the protected space *after* the computer is restarted – thereby modifying the condition of the data recited by claim 3. Applicant has amended claim 51 in a similar manner. As such, the recited language of claims 28 and 51 refines, rather than contradicts, the claims from which they depend and therefore meets the requirements of 35 U.S.C. § 112, second paragraph. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections to claims 28 and 51.

With respect to claim 69, the Examiner appears to assert that claim 69 is inconsistent with claim 67, from which it depends. As a preliminary matter, please note that the Applicant has amended claim 69 to correct typographical errors, which may clear up confusion as to its interpretation. The Examiner appears to base his conclusion of inconsistency on the assertion that claim 67 recites that "modification directed to unprotected data is written into the unprotected space directly," and that claim 69 recites "modification directed to the unprotected data is written to the redirected space instead of the unprotected space." (Office Action, p. 8.) However, claim 67 recites no such limitation. Specifically, claim 67 recites, "unprotected space designated on the storage device *for allowing modifications to a portion of the storage device*." The claim language is silent about the disposition of actual modifications directed to the unprotected space, as asserted by the Examiner. The disposition of modifications is described by dependent claims 68 and 69, which recite "disregarding" and "redirecting" accesses to the unprotected space, respectively. Accordingly, claims 69 and 67 are not inconsistent with each other.

Also, the Examiner appears to be arguing that claim 69 lacks support from the written description. However, if claim 69 is understood in context of related claims 67 and 68, as described above, claim 69 does not combine separate embodiments in a manner that is not supported by the written description, as asserted by the Examiner. The portion of the written description quoted by the Examiner states, "*In some embodiments*, when a portion of storage is indicated as unprotected, it is written to directly ... *In other embodiments*, the Redirection Driver redirects storage access requests to unprotected areas ..." (Office Action, p. 9.) As an initial matter, use of the language "in some embodiments" and "in other embodiments" merely describes two sets of embodiments that *may or may not* be disjoint. Furthermore, as is evident from the claim language, claim 67 recites a system having "unprotected space," and therefore describes the existence of unprotected storage areas that may be used for both embodiments described in the specification. Thus, that the "access requests to the unprotected space are also redirected" as recited in amended claim 69 describes an embodiment that uses the "unprotected space" recited in claim 67. As such, claim 69 is neither inconsistent with claim 67 nor unsupported by the written description. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection to claims 69.

Rejections Under 35 U.S.C. § 102

The Examiner has rejected claims 1-9, 11, 13-15, 30, 32-40, 50, 52-64, 66, 71-79, and 81-83 under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,832,263 issued to Hansen et al. ("Hansen"). The Examiner has also rejected claims 1-4, 27-29, 32, 50-52, 54-55, 67-68, 72, 79, and 83 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,092,161 issued to White et al. ("White").

Applicant respectfully traverses all these rejections for the reasons discussed in detail below.

The Examiner appears to be arguing that Hansen's described techniques, which describe a technique for providing an illusion of modifiability for otherwise non-modifiable storage devices, and/or White's described techniques, which provide a hardware supervisor for controlling access to and corruption of information in a computer system, somehow teach,

suggest, or motivate Applicant's claimed techniques for "providing a storage redirection driver that protects the storage devices of a computer system from alteration." (Specification, p.1, lines 11-12.)

Applicant respectfully disagrees for several reasons.

First, Applicant's claims recite several aspects that are nowhere taught, suggested, or motivated by Hansen. Each of independent claims 1-3, 32, 54, 72, and 79, recite receiving, intercepting, or otherwise processing requests that *would otherwise modify* a location in the designated protected space of a storage device. Specifically, claim 1 recites, "receiving a request for write access that would otherwise modify a portion of data on the storage device." Claim 2 recites, a "data access request that would otherwise modify an original location on the storage device." Claim 3 recites, "intercepting from requesting code a request that would otherwise modify a location in the protected space of the storage device." Claim 32 recites, "intercepting from requesting code a request that would otherwise modify a location in the protected space of the storage device." Claim 54 recites, "intercepts requests that would otherwise modify locations in the protected space." Claim 72 recites, "intercepting a request that would otherwise modify a location on the storage device." Claim 79 recites, "... intercepts a request that would otherwise modify one of the designated locations."

The Examiner appears to have improperly used Hansen as a basis for a rejection under 35 U.S.C. § 102, because Hansen does not describe "intercepting access requests that would otherwise modify a location on a storage device," (or similar language) as recited by Applicant's claims. The Examiner appears to suggest, in essence, that Hansen is apropos because the techniques described therein operate on physically non-modifiable storage (such as ROMs), non-modifiable storage as artificially imposed by an access control method, *and on modifiable storage*. (See Office Action, p. 6.) The Examiner further reasons that since the non-modifiable store ("NMS") of Hansen could be modifiable, the intercepting described by Hansen teaches Applicant's intercepting access requests "that would otherwise modify a location" on a storage device. However, contrary to what the Examiner asserts, there is nothing in Hansen to teach, suggest, or motivate that Hansen's techniques could operate on modifiable storage as used in a modifiable mode or are even of interest in that scenario. Rather, Hansen's techniques don't

make sense if the storage at issue is (based upon physical or access control) modifiable – there would be no need for Hansen's techniques to give the illusion of modification of non-modifiable storage because a write request could just actually modify the storage.

More specifically, the Examiner has constructed a scenario that is not described or suggested by Hansen, and has used that scenario as a basis for rejecting Applicant's claims. Examiner initially notes that the NMS ("Non-Modifiable Store") in Hansen may in some cases be not literally non-modifiable, such as when the characteristics of the underlying storage media permit modifications of information, but higher level abstractions (*e.g.*, an operating system, a file system, etc.) restrict modification to particular users or groups. (Office Action, p. 5.) From this premise, the Examiner draws the conclusion that there may exist circumstances under which an NMS may be modified, such as when a privileged user (*e.g.*, a system administrator) or an unauthorized user (*e.g.*, a hacker) attempt to write or otherwise alter the NMS. (Office Action, pp. 5-6.) Although one might imagine circumstances under which a particular type of user may alter information stored on an NMS, it does not follow that Hansen therefore teaches or suggests "intercepting access requests that would otherwise modify a location on a storage device," (or similar language) as recited by Applicant's claims. This is not a sufficient basis for a rejection under 35 U.S.C. § 102.

For a claim to be anticipated by a prior art reference under 35 U.S.C. § 102, the prior art reference must explicitly or implicitly describe every limitation of that claim. Although Hansen does describe non-modifiable stores that are not literally non-modifiable; for the purposes of the Hansen techniques, these stores <u>are</u> non-modifiable. (*See* Hansen, column 3, lines 49-53, hereinafter in column:line format). Hansen does not describe intercepting access requests for modifiable stores. Thus, Hansen cannot describe intercepting access requests "that would otherwise modify a location on a storage device," (or similar language) as recited by Applicant's claims. In particular, Hansen nowhere describes or suggests handling access requests issued by privileged and/or unauthorized users, such that those requests would actually result in a modification of a non-modifiable store, as suggested by the Examiner. (Office Action, pp. 5-6.) Accordingly, because Hansen does not describe processing or otherwise handling

requests that would *otherwise modify data* on a storage device, Hansen cannot anticipate Applicant's independent claims 1-3, 32, 54, 72, and 79 under 35 U.S.C. § 102.

Further, the modifications to Hansen suggested by the Examiner would not have been obvious to one skilled in the art at the time of that Hansen was filed. As an initial matter, Hansen contains no suggestion or motivation to modify its teachings in the manner suggested by the Examiner to include unauthorized users (hackers or otherwise) modifying the store or to apply its techniques to preventing modification of a store instead of giving the illusion of modification. Hansen nowhere describes *protecting* storage devices *from modifications* by any type of user or to a modifiable store. Hansen quite simply is not directed to obtaining such a goal. Examiner may not engage in hindsight reconstruction, using Applicant's claims as a template to attribute capabilities and features to Hansen other than what are explicit or even implicit in the reference and in the related prior art. As such, Hansen cannot teach, suggest, or motivate the modifications suggested by the Examiner.

Also, Hansen teaches away from any such modifications, because the modifications suggested by the Examiner are directly counter to the purposes of the techniques described by Hansen. As stated earlier, it doesn't make sense to modify Hansen to allow the illusion of modifying already modifiable storage because such a system doesn't really "do" anything. Hansen clearly states that it is an object of the invention to "provide a system and method for modifying information recorded in a *non-modifiable* store by intercepting file accesses and redirecting them based on whether originally stored information has been updated." (Hansen, 2:17-21, emphasis added.) Hansen further provides an explicit definition of the term *non-modifiable store*: "As used herein, "'non-modifiable store (NMS)' refers to *any storage which does not allow information or data to be changed* whether this limitation is imposed by a physical constraint of the storage media or artificially imposed as an access control method." (Hansen, 3:49-53, emphasis added.) By substituting the definition of non-modifiable store into the former passage, it is clear that the purpose of Hansen is to *modify* information recorded in a store that *does not allow* information or data to be changed, by intercepting file accesses and redirecting them. Hansen focuses explicitly on the concept of a non-modifiable store, as a

storage device that does not allow information or data to be changed. Thus, Hansen teaches away from intercepting requests to modifiable storage.

Furthermore, Hansen would be rendered inoperative for its intended purpose if modified as the Examiner suggests to intercept requests *to prevent modifications* by unauthorized or privileged users. The Examiner appears to suggest that the techniques described in Hansen (for intercepting and performing requests to a tracking store) would be equally applicable to protecting storage from unauthorized (*e.g.*, by a hacker) or inadvertent (*e.g.*, by a privileged user) modification. (Office Action, pp. 5-6.) However, the introduction of an unauthorized user renders Hansen inoperative for its intended purpose of intercepting and redirecting file accesses to NMS type of storage, because, in the presence of such users, non-modifiable stores are no longer actually (literally or non-literally, physically or logically) non-modifiable. Thus, because Hansen teaches away and/or is rendered inoperative if modified as the Examiner suggests, Hansen does not render obvious Applicant's independent claims 1-3, 32, 54, 72, and 79.

Second, Applicant's claims recite several aspects that are nowhere taught, suggested, or motivated by White. Each of independent claims 1-3, 32, 54, 72, and 79, recite a *redirection driver* or other software installed or loaded into memory. Specifically, claim 1 recites, "loading the redirection driver code into a memory of the computer system." Claim 2 recites, a "redirection driver, installed in the computer system during power-up initialization." Claim 3 recites, "software loaded into memory during power-up initialization." Claim 32 recites, "program code ... loaded into memory of a computer system during power-up initialization." Claim 54 recites, a "redirection driver, loaded into a memory of the computer system when the system is booted from a powered-down state." Claim 72 recites, a "installing a redirection driver ... in a calling sequence of the operating system." Claim 79 recites, a "redirection driver, installed in the computer system upon power-up initialization."

White, in contrast, does not teach, suggest, or motivate redirection drivers or other software components, as recited by Applicant's claims, let alone redirection drivers or other software components that perform the remaining aspects of Applicant's independent claims. In particular, White is directed to providing virus protection by way of a hardware and/or firmware supervisor that is preferably separate from a central processing unit of a computer system, and

that is capable of restricting read/write requests to a storage medium. (See, *e.g.*, White, 2:42-51, 3:24-32, and 4:12-20.) Significantly, White only describes *hardware* and/or *firmware* embodiments of the supervisor, and does not describe a *software* embodiment. For example, Figure 6 illustrates a "hardware arrangement suitable for implementing a first embodiment of a Supervisor." (White, 9:27-28.) Similarly, Figure 7 illustrates "a hardware arrangement suitable for implementing a second embodiment of a Supervisor." (White, 10:23-24.) Furthermore, Figure 8 shows "a schematic diagram of an actual embodiment of the Supervisor" that clearly depicts a *hardware* supervisor, as illustrated by the arrangement of Gate Array Logic devices, flip-flops, buffers, and ROMs. (White, 10:48-57.) White never describes a *redirection driver* or other software component as recited by Applicant's claims, let alone one for performing the other recited aspects of Applicant's claims.

Furthermore, if the supervisor of White were implemented as a software component, White would be inoperative for its intended purpose of virus protection. White describes an architecture that relies upon a supervisor microprocessor that is separate from a central processing unit of a computer system. (See, *e.g.*, Figures 6 and 7.) In the embodiments described by White, the supervisor microprocessor is implemented as hardware component that is external to a computer system and that reads executable instructions only from a dedicated read-only memory ("ROM"). These limitations appear necessary in order to protect the very operation of the supervisor from virus infection. With respect to Figure 6, White states, "a virus can never interfere with the Supervisor microprocessor 216 since it is *only* able to fetch executable code from its own ROM 213." (White, 10:16-18, emphasis added.) And again, with respect to Figures 7 and 8, White states that they "clearly [show] that a virus can never interfere with the Supervisor microprocessor 314 since it is *only* able to fetch executable code from its own ROM 326." (White, 11:27-29, emphasis added.) In short, White can only perform its function of protecting the computing system from viruses by virtue of the fact that it is implemented as an external hardware component that monitors and possibly restricts read/write requests to a storage medium. As such, White teaches away from using a redirection driver or other software component for its purposes or for the purposes recited by Applicant's claims.

Thus, because at least one aspect of claims 1-3, 32, 54, 72, and 79 is not taught, suggested or motivated by either Hansen or White, claims 1-3, 32, 54, 72, and 79 are not anticipated by or obvious in view of Hansen and/or White. Similarly, because dependent claims 4-9, 11, 13-31, 33-53, 56-71, 73-78, 80-81, and 83 incorporate the respective aspects of claims 1-3, 32, 54, 72, and 79 by virtue of their dependencies, the dependent claims also are not anticipated by or rendered obvious in view of Hansen and/or White, alone or in any motivated combination, for at least the reasons set forth above.

The Examiner has also rejected many of the dependent claims for different reasons. Applicant traverses these rejections and notes dependent claims 4-9, 11, 13-31, 33-53, 56-71, 73-78, 80-81, and 83 are also not taught, suggested, or motivated by either Hansen or White for a variety of additional reasons. For example, with respect to the rejection of claim 5, neither Hansen nor White teach, suggest, or motivate wherein "the driver is inserted into a driver hierarchy." Also, with respect to the rejection of claim 64, neither Hansen nor White teach, suggest, or motivate that the driver "refers to redirected space using multiple data addressing abstractions." In the interests of expediting prosecution, such arguments are not addressed in more detail herein. Accordingly, Applicant reserves the right to further traverse these rejections if necessary.

Conclusion

In view of the foregoing, Applicant submits that all of the claims in this application are allowable over the cited references. In the event the Examiner disagrees or finds minor informalities, Applicant respectfully requests a telephone interview to discuss the Examiner's issues and to expeditiously resolve prosecution of this application. Applicant's representative can be contacted at (206) 622-4900.

In closing, Applicant respectfully requests the Examiner to enter these amendments and to reconsider this application and its early allowance. The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090. Again, Applicant's representative thanks the Examiner for his prompt and courteous attention.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

Ellen M. Bierman

Ellen M. Bierman
Registration No. 38,079

EMB:asl

701 Fifth Avenue, Suite 6300
Seattle, Washington 98104-7092
Phone: (206) 622-4900
Fax: (206) 682-6031

808139_4.DOC